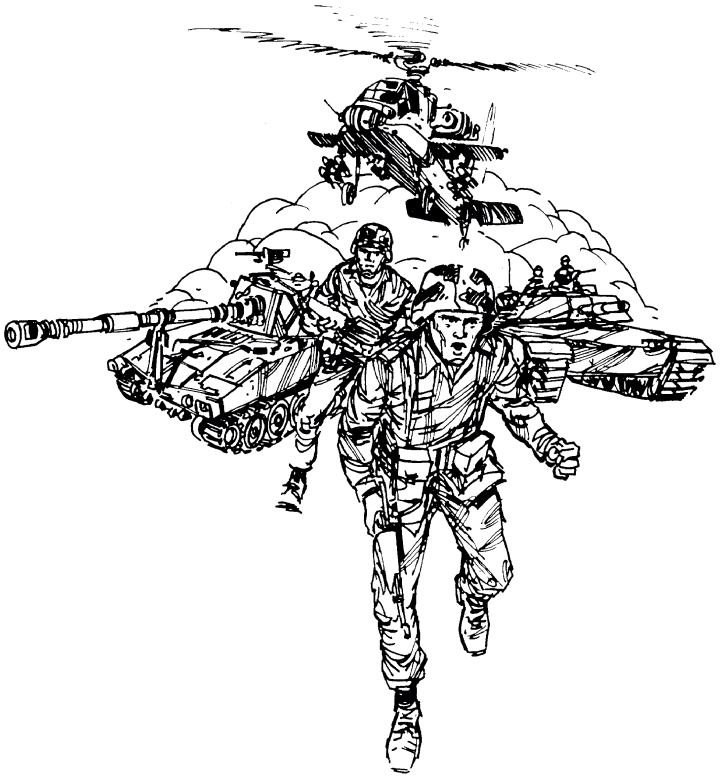
ARAT Bulletin

"Serving the Army Reprogramming Community Since 1994"

Volume 3, Issue 4 **February 1997**

Looking Back . . .Moving Forward



ARAT Perspective- Looking Back at 1996

The year 1996 was very productive for the ARAT project as it continued to expand its support to the ATSS community. The ARAT also saw several changes during that twelve month period.

One of the most significant changes during 1996 was in the leadership of the ARAT Project Office. Mr. Sok Kim, who had guided the project since 1993, took a leave of absence from the Government and passed the project responsibilities to Mr. Joseph Ingrao. Mr. Ingrao came in as no stranger to ARAT- his previous assignment was with the AEC Group in the CECOM Software Engineering Center.

With the Warfighter always first in the eyes of the ARAT, the Team provided direct support to U.S. aviators conducting operations in Bosnia and Korea. Relying on the latest BBS and WWW capabilities, the ARAT passed current Mission Data Sets which supported the latest threat detection technology in the hands of America's soldiers. *(cont. p. 3)*

In This Issue

From the Project Officer's Desk

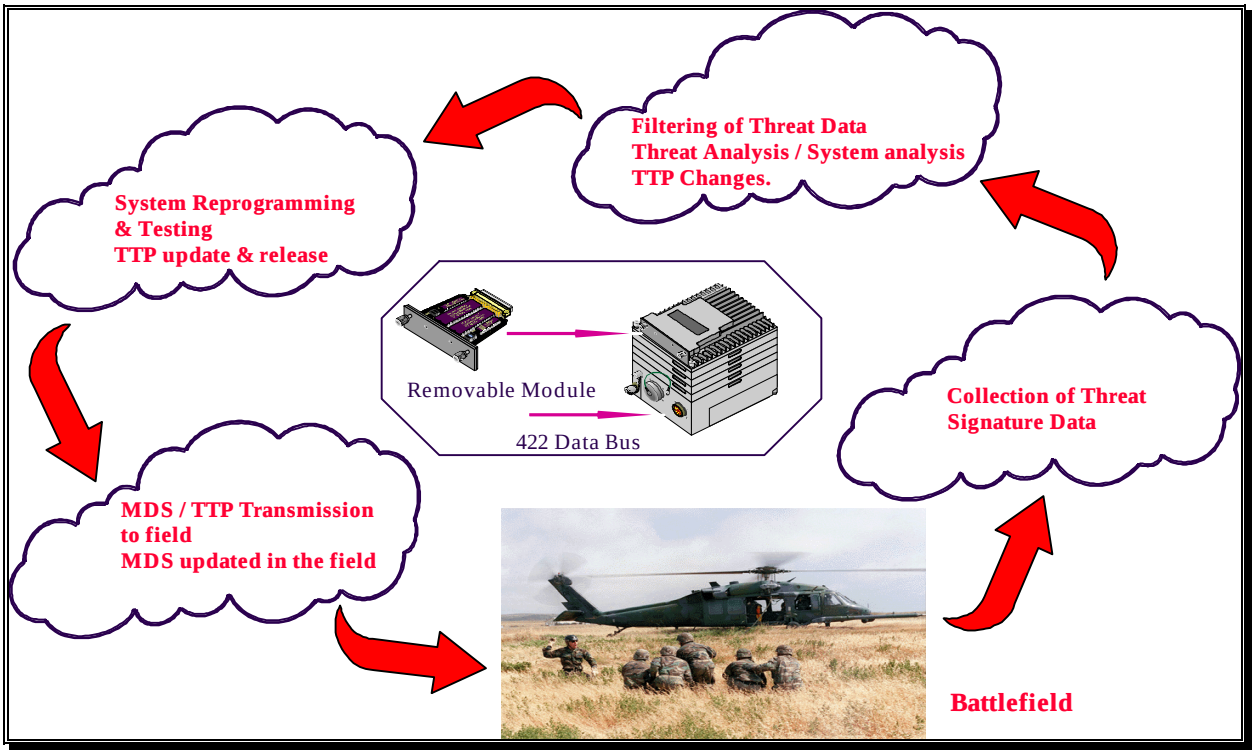
Information Operations, the Army's Been Doing It Since 1991 !!

Written by Mr. Joseph Ingrao, ARAT Project Officer

There have been many times I have seen the words "*Support the Warfighter*". I have the pleasure of working with a group of people who are really making a difference for the Warfighter. The ARAT's beginnings came from the hard learned and costly lessons we experienced in the Persian Gulf. A young LTC from DAMO-FDI was making the phrase "Support the Warfighters" more than just a slogan on the wall. He rallied support within the Army to activate an organization with the mission of actually applying the Army's lessons learned, instead of letting them sit in a database until the next military conflict arose. In 1991, MG Ronald Adams activated the ARAT to perform this mission and truly made the phrase "Support the Warfighter" mean something.

It has been one year since I took over the leadership of the ARAT Project Office from Mr. Sok Kim. It has been a time filled with excitement and challenge. The mission of this office is to provide a capability and infrastructure for our Electronic Warfare systems to be reprogrammed in a rapid manner. What this really means is to create a process and/or fix all the gray areas that fall in-between the collection of Information to the use of that Information in the field to support our Warfighters. Sounds like Information Operations? Well, it is. ARAT has been performing Information Operations for the Army's Target Sensing Systems since 1991.

My personal intentions for 1997 will be to have all the various components of the ARAT working together toward a common objective. That common objective is to have each member of the ARAT direct his individual efforts toward the final goal of developing the Information Infrastructure to *Support the Warfighter*.



Information Infrastructure

ARAT Perspective- Looking Back at 1996 (cont. from cover)

This past year saw an increased emphasis directed towards making the ARAT an established way-of-life for Army Warfighters. The ARAT conducted several visits and training conferences with Army Aviation Electronic Warfare Officers (EWOs) to expose the ARAT mission and accomplishments to a wider audience.

During 1996, the Memory Loader Verifier (pictured below) kit distribution program, to aid in downloading of Mission Data Sets (MDS), was accelerated to meet customer demands. The ARAT shipped over 50 kits to EWOs worldwide, with CECOM Logistics Activity Representatives (LARs) aiding ARAT by distributing the kits to EWOs in Bosnia and Korea, as well as at U.S. locations.

The kit, consisting of software and interface cable, gives the user the capability to download parametric changes from the Multi-Service Electronic Combat Bulletin Board System (MSECBBS) and upload these changes to mission helicopters in the battle zone prior to takeoff. This procedure represents a vast improvement over the reprogramming process used during Operation Desert Shield/Storm.

In 1996, the ARAT successfully tested its ability to support deployed Warfighters. With the cooperation of the U.S. Navy and Air Force, the ARAT, via INMARSAT satellite and the MSECBBS, passed reprogramming data between Eglin AFB and the USS Kennedy (CV-67) deployed in the Atlantic Ocean. With the tireless effort of Army EWOs in Korea, the ARAT completed a full cycle of the reprogramming process, from threat analysis through dissemination and uploading of changed MDS into aviation assets, during Exercise "Ulchi Focus Lens". This was the first time that the Army tested and evaluated the entire reprogramming process in a field environment.

Reprogramming at Sea- One of the highlights of 1996

The Foreign Military Sales (FMS) reprogramming effort for Allies and Coalition partners continued to increase as the ARAT team visited and trained technicians and aviation managers from five nations. Training focused primarily on the AN/APR39A(V)1 Radar Warning Receivers.

The ARAT project continued to support several conferences including the annual Electronic Warfare Integrated Reprogramming Data Base (EWIRDB) Conference. The ARAT hosted the conference which was held at Eglin AFB in May. An Association of Old Crows conference, also in May, saw the ARAT providing a simulation display of the MSECBBS to conference attendees. The ARAT also supported the Armed Forces Communications and Electronics Association (AFCEA) conference- *The World of C3 Today*. The ARAT again provided a capabilities display which received many visitors. One visitor in particular was the Honorable Emmett Paige,

Assistant Secretary of Defense for C3I, who showed an interest in the ARAT reprogramming efforts. At the Army Aviation Association of America (AAAA) convention in November, one of ARAT's own, Mr. Peter McGrew, was honored for his steadfast support to Army aviation. (See "Aviation Community Lands in New Jersey")

Several significant documents, listed below, were completed in 1996, which served as building blocks for the ARAT mission as the infrastructure is being developed:

- "System/ Segment Design Document for the Electronic Warfare Officer Support System (EWOSS)"
- "ATSS Rapid Reprogramming Process Guide"
- "The ATSS Rapid Reprogramming Project Plan, Revision #1"
- "ATRR Support Plan for Army Aviation TSS and Mission Planning Systems"
- "FMS Detailed Management Plan"
- "MLV Test and Evaluation Task Results"

The stage was set in 1996 for many ARAT initiatives. Armed with these developments, the ARAT can continue to provide timely support to its primary customer- The Warfighter.

Written by Mr. Verne Pedro, EPS, Inc.

Aviation Community Lands in New Jersey

Over 300 members of the Army's Aviation community gathered in Long Branch, New Jersey, last November as part of the Army Aviation Association of America (AAAA) Avionics and Electronic Combat (AEC) Symposium. Representatives from the ARAT-PO, ARAT-TA, ARAT-SE at Fort Monmouth, and the Fort Rucker ARAT-SC were part of this group which enjoyed three days of presentations and demonstrations focusing on emerging technology and issues affecting Army AEC.

The morning of the first day concentrated on addresses from key leaders in the Army's AEC and Research and Development communities. Featured speakers included MG Richard Stephenson (Ret.), President of AAAA, MG Gerard Brohm, Commanding General of the Army's Communications and Electronics Command, MG William L. Campbell, PEO Command, Control and Communications Systems, BG (P) David Gust, PEO IEW, Mr. Paul Bogosian, PEO Aviation, Mr. Robert Giordano, Director of the CECOM RDEC, and COL Roy Oler, PM AEC.

In his welcoming remarks, MG Stephenson emphasized the fact that everyone in the audience was "part of a digital revolution". MG Brohm echoed this sentiment when he stressed the application and synergy of Information Age technology in his keynote address.

Mr. Bogosian stressed many important requirements for supporting Army Aviators, two of which directly impact the ARAT community: the need to get technology into the field faster, and the need to rapidly react to changing electronic threat.

The highlight of the symposium's first day was the Awards Banquet held in the hotel. The evening featured a presentation by LTG Jay Garner, Assistant Vice Chief of Staff of the Army. LTG Garner focused on "Army Vision 2010" and the nation's continuing commitment to a Total Quality Force. The evening also featured the presentation of

the Association's ASE Award (pictured below) to Mr. Pete McGrew of the ARAT-TA, and the Avionics Award to SPC Verne Saint-Remy of the 6-101st Aviation Regiment, Fort Campbell, Kentucky.

AAAA ASE Award

Day Two of the symposium featured four professional sessions. These sessions focused on topics such as the Improved Data Module, Force XXI Software Logistics, the Battlefield Command Vehicle-Airborne, and Aviation Architecture Implementations and Support.

During the second session, Mr. Joseph Ingrao and Mr. Norman Svarrer, ARAT-TA, provided an overview of the ARAT Project. Their presentation centered on the history of the project, ARAT's integration into the Army and Joint Operations C4I environment, the Army reprogramming process, the application of the process to the AN/APR-39A(V)1, and the future focus of the project.

The last day of the symposium featured a classified session, held in the Meyer Center on Fort Monmouth, hosted by the Association of Old Crows. The topic of this session was "Electronic Warfare: Information Revolution for the 21st Century". The session concluded with a demonstration of the interaction of the AN/APR-39A(V)1 and the Suite of Integrated Infrared Countermeasures (SIIRCM) in identifying and engaging threats in a simulated environment.

A static display of the UH-60Q Medevac Helicopter in the parking lot of the Long Branch Hilton Hotel provided one of many symposium highlights

Also featured at the symposium was a technology display which featured the latest in AEC products and services. Members of the ARAT-PO support team staffed their own booth with working models of the AN/APR-39A(V)1, EWOSS Workstation, MLV, and ARAT Web Site.

Editor's Note: Those interested in reading "Army Vision 2010" can download a version from the Army Homepage at www.army.mil.

.

The ARAT Information Booth

Written by Mr. Joseph Skarbowski, Ilex Systems, Inc.

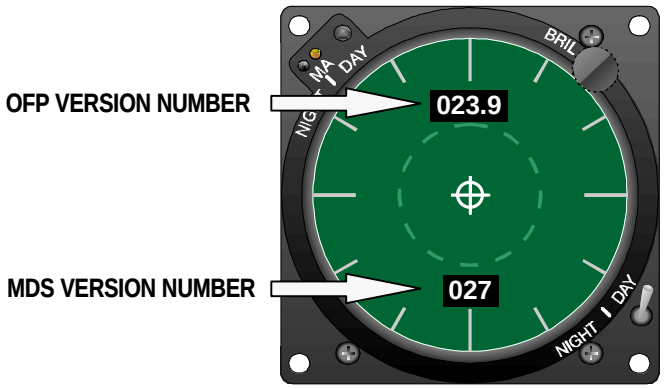
AN/APR-39A(V)1 OFP AND MDS NUMBERS: WHAT ARE THEY, WHAT DO THEY MEAN TO ME AS A USER ?

I am writing this article on a DELL Latitude Xpi 160MHZ computer loaded with Windows 95 Software (and wishing I had an Apple Power PC9500/200)- years ago I would have been content to use a Number 2 HB yellow pencil and some tablet-lined paper to write this epistle. As a military organization, we have become entranced with the importance of speed and having the most recent software (SW) for our professional and personal computers to improve our productivity and communicate our ideas better. Within the CECOM-SEC/NVESD/ARAT-TA network, we provide the most recent and usable software that will rapidly enhance the survivability of all those Army-lead AEC systems installed on the multiplicity of platforms both at home and with our allies around the world. I only hope that, in the case of all those deployed systems, the crewmembers using them are questioning/wanting the best software for their electronic combat systems that potentially could save their lives - just like they are probably doing right now in relation to their office PC and Apple machines !

Specifically, configuration management for the Army-lead AN/APR-39A(V)1 Radar Signal Detecting Set (RSDS) software resides within the purview of PM-AEC, CECOM-SEC and NVESD. Together this triumvirate determines what and when to field and to whom. What is to be fielded is software that has changed due to many factors e.g., anomaly rectification of previous versions, qualitative and quantitative improvements, expanding interfaces with other AEC systems, inputs from FMS and other customers to meet their specific needs, and changes due to threat emitter changes. When to field and to whom depends upon budgets, logistics, and operational requirements.

In discussing software and software numbers for the AN/APR-39A(V)1, there are two categories of software that we need to cover. They are the Operational Flight Program (OFP) and the Mission Data Set (MDS) - also previously known as the Emitter Identification Data (EID). This name changed in 1993 - we will tell you later what the changes encompassed are and why they better reflect the new name tag we have given it.

The AN/APR-39A(V)1 is the world's most widely deployed reprogrammable RSDS. When correctly powered up and crew-initiated Built-In Test (BIT) is activated, two sets of different numbers will be displayed at the twelve and six o'clock positions on the IP-1150A display.

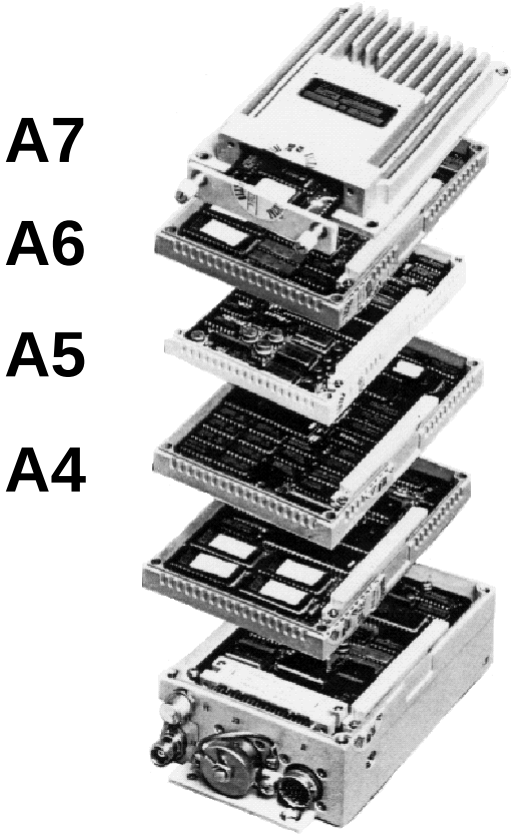


IP-1150A display of the AN/APR-39A(V)1

At the twelve o'clock position is the OFP Version Number- in this case it is the most recent Version Number: 023.9. At six o'clock is the MDS Version Number- in this case it is version 027 - built specifically for use at the National Training Center.

Let's take a minute and define what each specific software does in ensuring the optimal operation of the system. The OFP number identifies the installed SW version: this SW controls and manipulates how the processor (CP-1597) executes its operations. The OFP is the executive director of

all operations within the processor - this includes the scanning/sorting of the signal environment, making comparisons of the received emitter parameters with those loaded into the User Data Module (UDM), generating the correct symbology, and issuing the now famous synthetic audio commands. The software is both unclassified and classified. In computer 'geek' language look at the OFP as the operating software like Windows 95. The unclassified portion of the OFP is programmed onto Ultraviolet Programmable Read Only Memory (UV PROM) 8085 chips installed on the A4, A5, and A6 boards in the processor. The classified portion is programmed into Electronically Erasable Read Only Memory (EE PROM) Xicor 2864A chips and is resident on the A7 board or UDM of the CP-1597.



No doubt you 'old bold' experienced individuals have heard of other versions of both the OFP and MDS. After 1990 and prior to 1995 there were a number of OFPs that were deployed - the first and most widely deployed was 020.9. The reason others were deployed after this was to meet the expansion of additional requirements placed on the APR-39A(V)1 system. These additional but interim OFP versions were created to ensure other programs stayed on track e.g., AN/AVR-2/2A Laser Detecting Set, interface with AN/AAR-47 Missile Warning System, use with right/left receiver configuration, use with AN/APR-39(V)1 receivers to permit Foreign Military Sales (FMS) and last but not least, integration with the Longbow Apache. The OFP numbers in question were: 521.1, 021.2, 021.5 and 022.2. Today, one version of the OFP software encompasses all these changes - it is 023.9. So if you have any other version than this installed in your platform or hidden away in your 'goodie' locker you need to make arrangements to get it changed - ASAP. We will discuss the reasons why a little bit later.

The MDS has seen and will see more number changes than the OFP. The first deployed MDS (then EID) was 017 (Global EID)- today we have seen over 20 numbers to include our FMS and specialty customers. For U.S. users of the AN/APR-39A(V)1 system, the MDSs that are operational and available are stored aboard the secure Multi-Service Electronic Combat Bulletin Board System (MSECBBS): jointly operated by the Services out of Eglin AFB. Each MDS has been tailored for a specific geographical area and platform mission profile. These MDSs are living breathing SW packages - subject to change - that reflect the environment at a particular time. As we all know, countries buy new weapon systems and discard old ones - thus the environment or order of battle in which our operators use the AN/APR-39A(V)1 system is dynamic and ever changing. Due to limitations in budget and the time delay in enhancing these systems with hardware updates, the US Army relies extensively on its changes to be incorporated in the SW arena. From the threat perspective it is the ARAT-TA that triggers the CECOM-SEC/NVESD/PM-AEC organizations to such changes when and if countries update their

weapon inventories, e.g. Peru with the purchase of MIG-29s(1), and Thailand's purchase of Giraffe radars(2).

Although the OFP is constantly being reviewed for efficiency, it is normally only planned to be updated, on average, every two-three years. As the OFP is stored in UVPROMS on the cards, it is significantly more challenging logistically to capture and change each one. Thus the OFP block cycle update has to be thoroughly planned, tested and executed in a coordinated manner to ensure that a base standard is set across the board for all users. The SW that has the potential to change the most (and it does) is the MDS. We know that this RSDS was built in an era when emitter fingerprints were not quite as complex and threats not as widely deployed. We also know from experience that if you 'cram' too much information into its memory it becomes less effective in presenting a more realistic threat identification (i.e., more chance for ambiguity). That is why the U.S. Army is leading the way in which it theaterizes or geo-tailors data for customer use. This higher fidelity means that there are more MDSs for use - but more importantly - that the user community knows which one to use and for where!

With this philosophy established, additional requirements came for both the CECOM-SEC and ARAT-TA. Even though the data loaded into the UDM was just 'ones and zeros' it was incumbent upon the organizational structure to define exactly what each MDS was, where it was to be used, what it was to be used for, what symbology was to be used for display, and any other pertinent capabilities and limitations for its use in a particular scenario or theater. This increase in data available to the user is why the ARAT-TA opted to change the name from Emitter Identification Data (EID) to MDS - because to be effectively used, the operators need to know more than just the basics! Thus the MDS files that are loaded onto the MSECBBS in the AN/APR-39A(V)1 Library are executable files, e.g., MDS040.exe. Once you download this file and open it up, the file 'explodes' into six individual files - in other words a data set. These files are listed below:

040list.txt	This file provides a list of the emitters in priority sequence with associated IP1150A display symbols
040notes.txt	This file is known as the pertinent notes file. It contains expanded information on the threats, to include the ELINT Notations(ELNOTS), the geo-tailored area of operations for this specific MDS and any limitations that the MDS might have regarding detection and identification.
040hex.udm	This file is for use when using a memory loader verifier to upload to the CP-1597.
040hex.hex	This file is used when uploading to the CP-1597 through the use of a laptop/PC and the upload cable provided by the ARAT Project Office.
040flag.txt	This file is used by the ARAT engineers collocated at the Air Force Information Warfare Center who manage the RSDS flagging models.
040knee.ppt	This file is a new addition and is a pictorial presentation of the kneeboard card. Data presented is the emitter, symbology and associated priority. To view this file, MS Powerpoint 4.0 or newer is required.

As I mentioned earlier, the MDSs are the 'volatile' SW packages. The only way to know what is available and for what area of the world is to become a subscriber to the MSECBBS. The U.S. Army (CECOM-SEC/NVESD and PM-AEC) can no longer afford to go out to each unit location, find all the platforms and load and verify each MDS. The flexibility of today's Army operations has forced the unit level to become responsible for its own 'EW destiny' - in ensuring that the ASE systems installed on their platforms are optimized

for their mission with the best SW available. To do this for the AN/APR-39A(V)1, just press BIT, then check the OFP and MDS. Ask your unit Electronic Warfare Officer if the MDS number is correct. If the OFP does not read 023.9, then you are missing out on some major SW advances that improve signal recognition and the ability to upload new MDSs via electronic means at the unit level.

As a final note: if you find that you have an 'old' OFP processor number, you can call PM-AEC-LM or CECOM-NVESD to find out how to dispose of it and have it replaced with the newest OFP. If you are not a MSECBBS subscriber you can call ARAT-TA and we can assist you in getting aboard to get you that most recent MDS.

References:
(1) Aviation Week and Space Technology 02 December 1996 P25-26.
(2) Microwave Journal September 1996 P41.

Written by Mr. Pete McGrew, SRI International

Another Means to Accessing the MSECBBS

Traditionally, if you want to gain access to the Multi-Service Electronic Warfare Bulletin Board System (MSECBBS), you had one option. That option was to make a telephone call to the MSECBBS at Eglin AFB, FL, via a CS3 accredited computer, running Procomm Plus for Windows or another similar communications application, connected to a Secure Telephone Unit (STU-III). Now, there is an alternate means to get to the MSECBBS - access via the Transmission Control Protocol/Internet Protocol (TCP/IP)-based "Secure Internet Protocol Router Network" (SIPRNET), the Government's Secret-Collateral version of the "Internet".

There are several ways to attain access to the SIPRNET. You can choose which one of the following to use depending on what resources are available to your particular situation:

- Option #1- You can request a direct SIPRNET circuit from the Defense Information Systems Agency (DISA). This option requires that you incur a one-time hookup charge and a monthly circuit cost. Contact your local Directorate of Corporate Information (DCI) representative for additional details.

- Option #2- You can inquire of your local DCI staff if there is a SIPRNET circuit somewhere on your post, base or camp. If so, you may be able to make arrangements with the agency which has this circuit to extend access to you, or at least allow you to physically visit their facility to gain access to the SIPRNET.

- Option #3- You can request dial-up STU-III access to the SIPRNET from the ARAT-PO. To do so, you need to complete and return an "ARAT Account Application". For your convenience, a blank form is enclosed in this issue of the "ARAT Bulletin".

  This option does have one drawback, however. It will only be feasible if you are able to make a telephone call to the Continental United States (CONUS). You will need to run, on your accredited computer, TCP/IP software that provides Point-to-Point Protocol (PPP) capability. The ARAT-PO can provide guidance on how to attain the necessary software and with configuring your computer.

- Option #4- You can obtain dial-up STU-III access to SIPRNET from DISA. This benefits OCONUS users, as DISA has "Comm Servers" at several locations throughout the world, which permit OCONUS users to make "local" rather than long distance calls. These "Comm Servers" provide a direct access to SIPRNET,

- thereby eliminating the need to make a sometimes difficult, and unreliable, telephone call to CONUS for OCONUS users.

To qualify for this option, DISA requires that the user be "sponsored" by a registered organization on the SIPRNET that can provide the user with an e-mail account. The ARAT-PO can provide this capability to members of the Reprogramming Community. Those desiring DISA dial-up access should fill out an "ARAT Account Application" as well as a DISA "SIPRNET User Registration Form" (also enclosed) and submit them both to the ARAT-PO.

For those users who do not yet have MSECBBS accounts, please note that applying for ARAT and DISA "Comm Server" accounts is separate from applying for MSECSBBS access. For access to the MSECBBS, prepare a memorandum (refer to enclosed example) and submit it to the MSECBBS System Operator. Mail that memorandum directly to the address shown on the example.

If needed, blank forms and instructions are also located on the unclassified ARAT WWW Site at URL:

http://arat.iew.sed.monmouth.army.mil /ARAT/ forms/forms.html.

Written by Mr. Andrew Lombardo, Ilex Systems, Inc.

SIPRNET User Registration Form 4/96
Do Not Change Format - Enter Data Here

U1A. SSC Handle: <Leave Blank>
U1B. Delete User: <Leave Blank>

NAME INFORMATION:
U2A. Last Name: Doe
U2B. First Name: John
U2C. Middle Initial: Q.
U2D. Name Suffix: IV
U2E. Title/Rank: CW2

ADDRESS INFORMATION:
U3A. Address Line 1: HHC, 1/23 AVN BN
U3B. Address Line 2: ATTN: AMLBB-AVN-123-S3-EW
U3C. Address Line 3: Bldg. 121
U3D. Address Line 4: -----
U3E. City or APO or FPO: Ft. Swampy
U3F. State or APO/FPO: AR
U3G. Zip Code: 12345

PHONE INFORMATION
PRIMARY PHONE
U4A. COMMERCIAL PHONE: 999-530-1234
U4B. COMMERCIAL PHONE EXTENSION: 111
U4C. DSN PHONE: 123-4567
U4D. DSN PHONE EXTENSION: ---
U4E. FAX PHONE: 999-530-1969
ALTERNATE PHONE
U4A. COMMERCIAL PHONE: 999-530-4321
U4B. COMMERCIAL PHONE EXTENSION: 121
U4C. DSN PHONE: 123-4321
U4D. DSN PHONE EXTENSION: ---
U4E. FAX PHONE: 999-530-6919

E-MAIL INFORMATION:
U5A. E-Mail Address:
doe@arat.army.smil.mil
U5B. Host Administrator Handle: <Leave Blank>
U5C. Additional E-mail Address:
<fill in if you already have a SIPRNET email address>

COMM SERVER ACCESS CARD INFORMATION
U6A. LAA ORGID: <Leave Blank>
U6B. LAA Administrator Handle: <Leave Blank>
U6C. Issue Card? (N,R,P): N
U6D. Terminate Access: <Leave Blank>
U6E. Reason? <Leave Blank>

COMSEC ACCOUNT INFORMATION
U7A. COMSEC Account Number: XXX123
U7B. Organization PLA:
CDR 10 AD/AVN/123//

ADDRESS INFORMATION
U7C. Commander
U7D. 1/23 AVN BN
U7E. ATTN: AMLBB-AVN-123-CE
U7F. Bldg. 121
U7G. Ft. Swampy
U7H. AR
U7I. 12345

How to Apply

Applying is simple. Fill out the "ARAT Account Application" form and submit it through the mail, unclassified fax, or unclassified e-mail (with follow-on hardcopy within seven days) to the ARAT-PO. If you need to establish connectivity through a DISA "Comm Server", fill out a DISA "SIPRNET User Registration Form" and submit it to the ARAT-PO with your the "ARAT Account Application". The ARAT-PO will submit the "SIPRNET User Registration Form" to the DISA SIPRNET Office at Fort Huachuca, AZ, on your behalf. Do not send this form directly to DISA because there is information which the ARAT-PO must provide before the form goes forward. Once approved, DISA will send instructions and a separate STU-III Crypto Ignition Key (CIK), for use in connecting to their "Comm Servers", to your COMSEC Officer within approximately 30 days.

More Than Just An Alternative

Access to the SIPRNET not only provides an alternate route to MSECBBS, but also opens many other doors to members of the Reprogramming Community. The ARAT has a web site accessible through SIPRNET. Many of the National Intelligence Agencies (DIA, CIA, NSA), Unified Command CINC's (CENTCOM, ACOM, EUCOM, etc.), and Service-intelligence agencies (NGIC, NAIC, etc.) also provide valuable information from their SIPRNET web sites. To join in on the action, obtain access to the SIPRNET though one of the options you just read. Submit your "ARAT Account Application" and/or "SIPRNET User Registration Form" to the ARAT-PO for processing. If you have any questions beforehand, you may contact Mr. Ken Kragh, ARAT-PO SIPRNET POC, DSN: 992-6003, Commercial 908-532-6003, or unclassified e-mail: kragh@doim6.monmouth.army.mil.

Don't be left out. Apply today!!

ARAT ACCOUNT APPLICATION (EXAMPLE)

Instructions for Opening an ARAT Account:

1. Completing the Form:
(A) Fill in your personal information and sign the form after reading the certification statements.
(B) This section is filled out only if you are a contractor with a mission requirement to access the ARAT network. Attach a copy of the DD Form 254, Contract Security Classification, obtained from your company Facility Security Officer (FSO). Your FSO should have the requested information.
(C) This section is completed by either the ARAT-PO, your First-Line Supervisor, Security Officer/Manager, or the contract Project Manager.
(D) Indicate which systems/services you are requesting access to.
(E) This section is completed by your Security Officer/Manager.
(F) This section is completed by your Information Systems Security Officer/Manager. Attach a copy of the computer's approved security accreditation.
(G) This section is completed by the ARAT Network Administration Team during the account creation process. Leave blank.
(H) Include any additional remarks as appropriate.
(I) To submit the application for processing, follow the Mail/Fax instructions as stated. To speed up processing time, you can email the account form to the below POC, however, originals of each form must follow in the mail within a week or the account access will be suspended.
2. You will be notified of your account's userid and password within a week by the ARAT-PO.
3. Contact the ARAT-PO for further assistance and information. POC is Mr. Ken Kragh, ARAT-PO, DSN 992-6003, CML (908) 532-6003, unclassified email: kragh@doim6.monmouth.army.mil

A. Applicant Information

Last Name, First Name, MI	Rank/Grade	SSN
Doe, John Q.	**CW2**	**123-45-6789**

Status: Active Military Reserves Nat'l Guard Government Civilian Contractor	Position Description/Job Title
XXX	**Battalion EWO**
Organization (add company name if contractor)	Office Symbol
HHC, 1/23 Aviation Battalion	**AMLBB-AVN-123-S3-EW**
Organizational Address (Include Zip Code)	Phone (Indicate DSN/CML/STU-III)
Bldg 121, Ft. Swampy, AR 12345	**CML (999) 530-1234, ext 111, DSN 123-4567 (STU-III)**
Unclassified email address	Classified email address (indicate whether on SIPRNET or JWICS)
doe@amlbb.123.army.mil	**doe@amlbb.123.army.smil.mil (SIPRNET)**

I, the requestor/user, certify that:
1. The computer account will used in support of an official government project/contract.
2. All actions related to use of this account and its inherent access to classified Department of Defense computer systems will be governed by all applicable security regulations, policy directives, and guidelines in existence.
3. I will only access the ARAT network via an accredited (up to SECRET Collateral) computer and will safeguard the classified data contents of this account, my computer, and the security of the applicable associated cryptographic material. (Attach a copy of the computer's security accreditation.)
4. I will not willfully compromise the account password. (Examples of willful compromise include storing account password in a PC or terminal; developing automatic login procedures that circumvent the manual entry of the account's username and password; or, allowing anyone, without first executing the proper need-to-know, to use the account.)
5. I will notify ARAT-PO when the account is no longer needed, when account information needs to be revised, or the password has been compromised.
6. I will coordinate password changes with the ARAT network administration team semiannually.

Signature	Date
/s/ Doe, John Q.	**8 JAN 97**

B. Contractor Applicant Additional Information (Facility Security Officer - attach copy of DD Form 254)

Company Facility Clearance	Cage Code	Contract Number	Contract Expiration Date

C. Need-to-Know Certification (ARAT-PO, First-Line Supervisor, Security Officer/Manager, contract Project Manager)

I certify that the applicant has the proper need-to-know to be granted an account on the ARAT network/server, and to access the classified (SECRET collateral) Secure Internet Protocol Router Network (SIPRNET) and all its affiliated services (Email, INTELink-S World Wide Web, News).

Name/Title/Organization (include relationship to Applicant)	Signature	Date
Ken Kragh, ARAT, Project Manager		**8 JAN 97**

D. Request Access to the following Systems/Services ('X' all that apply):

SIPRNET/INTELink-S WWW Access:		CIK ID (STU-III Key)	STU-III Make/Model
Local Facility (Rm 226, Bldg 1210)	Remote Dial-up PPP via STU-III ==> **X**	**123456789**	**AT&T 1100**

Services		Theater of Responsibility (Be as specific as possible, i.e. Korea within PACOM):						
SIPRNET Email account	WWW Threat Data ==>	ACOM	CENTCOM	EUCOM	NTC	PACOM	SOUTHCOM	Other
X	**X**		**IQ**					

ARAT-PO Form 1, 1 JAN 97 (Page 1 of 2)

ARAT ACCOUNT APPLICATION (EXAMPLE)

E. Security Clearance Certification (Security Officer/Manager)

I certify that the applicant has a minimum of a Secret Collateral security clearance.

Type of Investigation	Degree of Clearance	Granted By	Granted On
BI	**SECRET**	**CCF**	**8 JAN 97**

Name/Title/Organization	Signature	Date
Jack Mack, CPT, MI, Battalion S-2	**/s/ Jack Mack**	**8 JAN 97**

F. Computer Accreditation Certification (Information Systems Security Officer/Manager - attach copy of accreditation)

I certify that the applicant has a computer accredited at the CS3 level to access the Secure Internet Protocol Router Network (SIPRNET).

Computer Accreditation Level	Granted By	Granted on
CS3	**FSO**	**8 JAN 97**

Name/Title/Organization	Signature	Date
Jack Mack, CPT, MI, Battalion S-2	**/s/ Jack Mack**	**8 JAN 97**

G. ARAT Network Administration Actions (for ARAT-PO internal tracking use only)

Date Form Received	Received By	Approved By

System Account User Name	System Server	Date Created	Created By	Date Deleted	Deleted By

H. Additional Remarks

None.

I. Completion Instructions

Mail Completed Form and appropriate attachments to:
MR. KEN KRAGH
US ARMY CECOM SOFTWARE ENGINEERING CENTER
ATTN: AMSEL-RD-SE-SY-AI-CM (ARAT)
BUILDING 1210, RITTKO AVENUE
FORT MONMOUTH, NJ 07703-5207

Or FAX to: DSN 992 - 5238 / CML (908) 532 - 5238
Alternate: DSN 992 - 4621 / CML (908) 532 - 4621
Address Fax to: ATTN: ARAT, Mr. Ken Kragh
Both Faxes operate 24 hours/day, 365 days/year
Or email to: kragh@doim6.monmouth.army.mil
Follow up with originals via mail or fax within a week.

ARAT-PO Form 1, 1 JAN 97 (Page 2 of 2)

Notes to the Field

Special Farewell

LTC Don Adkins, Officer-In-Charge (OIC) of the ARAT Threat Analysis Center, is currently receiving additional flight training in preparation for his new assignment as the Commander of the 3d Military Intelligence Battalion (Aerial Exploitation) at Camp Humphreys, Korea. LTC Adkins' wisdom and determination have been instrumental to the success that the ARAT program enjoys today. We are confident that not only will he do a superlative job leading some of the finest Aviators in the U.S. Army, but he will also continue to be a champion of all that ARAT brings to the ATSS Community. We want to send Don and his family best wishes for a successful command and an enjoyable tour in the "Land of the Morning Calm".

Lessons Learned

The ARAT-PO continues to collect Army Reprogramming Lessons Learned. If you have experienced a reprogramming related problem and could not find a solution, or maybe you did find a solution which no one else thought of, or found a better way of doing a procedure, submit it to the ARAT-PO. The problem does not have to be during an exercise or contingency operation. In fact, if we can deal with the problem before an exercise or contingency operation, the better off we will be in the long term.

Send your unclassified Lessons Learned to:

Commander, USACECOM
ATTN: AMSEL-RD-SE-SY-AI-CM
Building 1210
Fort Monmouth, NJ 07712
-or-
Fax to: DSN 992-5238 (u) (Com. 908-532-5238)

Send classified Lessons Learned to:

Commander, USACECOM
ATTN: AMSEL-RD-SE-S
Building 1210
Fort Monmouth, NJ 07712

(Enclose an annotation that the material is to be forwarded to the ARAT-PO.)

Call for Articles

The staff of the "ARAT Bulletin" would like to hear from you, the Warfighter. We would like to publish your ideas, adventures and lessons learned so that all may benefit from you expertise and experiences.

We are interested in, but not limited to, unclassified articles for the following topics:

- Reprogramming Lessons Learned (include the problem and solution/workaround)
- Reprogramming-related conferences and training sessions
- Current or emerging ATSS

Submit your manuscript (both hardcopy and on a 3 ½" disk in MS Word 6.0 or .TXT format) to the ARAT-PO. There is no deadline; we will review all articles and publish them on a pertinence/space-available basis.

You have read our articles for the past three years, now it is your turn. Our goal is to use the "ARAT Bulletin" as a tool which serves as a medium for information exchange within the Army (and Joint) reprogramming community.

For Your Information

Coming Events

Association of Old Crows "Fiesta Crow" Convention	San Antonio, TX	20-23 April 1997
EWIRDB Conference	San Antonio, TX	21-25 April 1997
1997 AAAA National Convention	Louisville, KY	23-26 April 1997

The ARAT Community
Key Points of Contact

HQDA, DAMO-FDI	Mr. Rick Simon	DSN: 227-6527 FAX: 223-5336
HQ, TRADOC	Mr. Bob Miner minerr@emh10.monroe.army.mil	DSN: 680-2664 FAX: 680-2947
HQ, INSCOM	COL Halbert Stevens	DSN: 235-1791 FAX: 656-1003
ARAT-PO	Mr. Joseph Ingrao ingrao@doim6.monmouth.army.mil	DSN: 992-1337 FAX: 992-5238
	Mr. Ken Kragh kragh@doim6.monmouth.army.mil	DSN: 992-6003 FAX: 992-5238
ARAT-TA	LTC Donald M. Adkins adkinsd@wg53.eglin.af.mil	DSN: 872-8899 FAX: 872-8213(C) /4268(U)
	Mr. Norm Svarrer svarrer@wg53.eglin.af.mil	DSN: 872-8899 FAX: 872-8213(C) /4268(U)
ARAT-SE (CECOM)	Mr. Jeff Boldridge boldridj@doim6.monmouth.army.mil	DSN: 992-8224 FAX: 992-8287
ARAT-SE (MICOM)	Mr. Gary Clayton clayton-rd-ba@redstone-emh2.army.mil	DSN: 746-0755 FAX: 746-0757
ARAT-SC (FT. BLISS)	Mr. Ernesto Martinez martinem@bliss-emh1.army.mil	DSN: 978-5595 FAX: 978-2773
ARAT-SC (FT. RUCKER)	Mr. George Hall hallg@rucker-emh3.army.mil	DSN: 558-9334 FAX: 558-1165
AFIWC (KELLY AFB) (Army Flagging)	Mr. Carl Brunner cbrunner@sdd.sri.com	DSN: 969-2021 FAX: (210) 977-2145

The ARAT Bulletin Staff	
Editor-In-Chief Mr. Joseph Ingrao, ARAT Project Office **Editors** Mr. Joseph Skarbowski, Ilex Systems, Inc. Mr. Samuel Johnson, Ilex Systems, Inc.	Send comments, changes of address, and articles to: Commander, USACECOM ATTN: AMSEL-RD-SE-SY-AI-CM Building 1210 Fort Monmouth, NJ 07712